FITZGERALD MONROE FLYNN PC
JACK FITZGERALD (SBN 257370)
jfitzgerald@fmfpc.com
MELANIE R. MONROE (SBN 275423)
mmonroe@fmfpc.com
TREVOR FLYNN (SBN 253362)
tflynn@fmfpc.com
PETER GRAZUL (SBN 342735)
pgrazul@fmfpc.com
ALLISON FERRARO (SBN 351455)
aferraro@fmfpc.com
2341 Jefferson Street, Suite 200
San Diego, California 92110
Phone: (619) 215-1741
Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

NATASSIA TIMOTHEE, TOMMY DIEP, ESPERANZA REYES, MARIAELENA BURCIAGA, and STACY PENNING on behalf of themselves, all others similarly situated, and the general public,

Plaintiffs,

v.

META PLATFORMS, INC., SACRAMENTO FOOD BANK AND FAMILY SERVICES, LOS ANGELES REGIONAL FOOD BANK, CENTRAL CALIFORNIA FOOD BANK, and SAN FRANCISCO FOOD BANK d/b/a SAN FRANCISCO-MARIN FOOD BANK,

Defendants.

Case No: 25-cv-5106

CLASS ACTION

COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs NATASSIA TIMOTHEE, TOMMY DIEP, ESPERANZA REYES, MARIAELENA BURCIAGA, and STACY PENNING, on behalf of themselves, all others similarly situated, and the general public, by and through their undersigned counsel, bring this action against Defendants META PLATFORMS, INC. ("Meta"), SACRAMENTO FOOD BANK AND FAMILY SERVICES, LOS ANGELES REGIONAL FOOD BANK, CENTRAL CALIFORNIA FOOD BANK, and the SAN FRANCISCO FOOD BANK d/b/a SAN FRANCISCO-MARIN FOOD BANK (collectively, the "Food Bank Defendants"), and allege the following upon their own knowledge, or where they lack personal knowledge, upon information and belief, including the investigation of their counsel.

INTRODUCTION

1. The Food Bank Defendants are 501(3)(c) non-profit organizations that help those experiencing financial hardship access food and financial assistance.

2. In violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et. seq.* ("CIPA"), the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et. seq.* ("CCPA"), the Electronic Communications Privacy Act , 18 U.S.C. §§ 2510 *et seq.* ("Wiretap Act"), the common law right to privacy, and California's Constitutional Right to Privacy, among other laws, the Food Bank Defendants incorporate Meta's tracking technology, the Meta Tracking Pixel ("Pixel"), on their websites, which they know allows Meta to contemporaneously intercept, and subsequently sell, vast quantities of users' sensitive financial and personal information, including medical information, without their knowledge or consent.

3. Meta (formerly known as Facebook) offers to website owners the Pixel, which allows owners to track users' actions on their websites, and measure the effectiveness of advertising, by adding the Pixel's source code to their websites. When embedded on a third-party website, the Pixel tracks each user's activity on that website and sends that data to Meta, linking this information with users' personal identities.

4. Through the Pixel, Meta collects information such as visited websites and user interactions with content, allowing Meta to build detailed user profiles. Over time, as the Pixel collects more data, Meta can refine and expand the user profile, enabling it to serve highly-targeted advertisements based on a user's habits and preferences, for its own profit.

5. For example, the Pixel can track and log each page a user visits, what buttons they click, and the specific information they input into the website, such as user-generated inputs into forms regarding their

financial status, or need for vulnerable-status-based financial assistance. The Pixel contemporaneously takes each of these pieces of information and sends it to Meta with personally identifiable information ("PII"), such as the user's IP address and location, name, email, or phone number, to connect the information to the specific user's Facebook or Instagram profile. Meta stores this data on its own server, in some instances, for years, and discloses, shares, and sells this data to other third parties for profit.

6. All Food Bank Defendants have incorporated the Pixel onto their websites. The Food Bank Defendants' inclusion of the undisclosed Pixel on their websites caused Plaintiffs' and other Class Members' confidential communications, PII, and sensitive financial information to be intercepted by and sent to Meta. Plaintiffs and other Class Members did not consent to the Food Bank Defendants sharing this sensitive information with Meta or any other third parties, including for targeted advertising. The Food Bank Defendants knew that by embedding their websites with the Pixel, they were permitting Meta to intercept and use Plaintiffs' and other Class Members' PII, including sensitive financial information.

7. Meta's designing and furnishing of the Pixel, an eavesdropping device, to the Food Bank Defendants allowed it to intercept Plaintiffs' and other Class Members' PII, confidential communications, and sensitive financial information, for the improper purpose of selling the information to third-party advertisers without Plaintiffs' or other Class Members' consent.

8. The actions of the Food Bank Defendants and Meta constitute an extreme invasion of Plaintiffs' and other Class Members' right to privacy and violate state statutory and common law.

JURISDICTION & VENUE

9. The Court has original jurisdiction over this action under 28 U.S.C. § 1331 because it is a civil action arising under the laws of the United States, specifically 18 U.S.C. § 2510 *et. seq.* (the Electronic Communications Privacy Act), and the Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

10. Alternatively, the Court has original jurisdiction over this action under 28 U.S.C. § 1332(d)(2) (The Class Action Fairness Act) because the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interests and costs, and at least one member of the class of plaintiffs is a citizen of a State different from the Defendants.

11. The Court has personal jurisdiction over Sacramento Food Bank and Family Services because it has purposely availed itself of the benefits and privileges of conducting business activities within California. Sacramento Food Bank and Family Services operates in Sacramento County, California.

12. The Court has personal jurisdiction over Los Angeles Regional Food Bank because it has purposely availed itself of the benefits and privileges of conducting business activities within California. Los Angeles Regional Food Bank operates in Los Angeles County, California.

13. The Court has personal jurisdiction over Central California Food Bank because it has purposely availed itself of the benefits and privileges of conducting business activities within California. Central California Food Bank operates in Fresno County, California.

14. The court has personal jurisdiction over San Francisco-Marin Food Bank because it has purposely availed itself of the benefits and privileges of conducting business activities within California. San Francisco-Marin Food Bank operates in San Francisco County and Marin County, California.

15. The Court has personal jurisdiction over Meta Platforms, Inc. because it resides in this district.

16. Venue is proper in this Northern District of California pursuant to 28 U.S.C. § 1391(b) and (c), because Meta Platforms, Inc. resides in (*i.e.*, is subject to personal jurisdiction in) this district, and because a substantial part of the events or omissions giving rise to the claims occurred in this district.

DIVISIONAL ASSIGNMENT

17. This civil action arises, in part, out of the actions and omissions of Meta which occurred in San Mateo County. Therefore, pursuant to Civil Local Rule 3-2(c) and (d), this action is correctly assigned to the San Francisco or Oakland Division.

PARTIES

18. Plaintiff Natassia Timothee is a California citizen over 18 years of age who resides in and intends to remain in Sacramento County, CA.

19. Plaintiff Tommy Diep is a California citizen over 18 years of age who lives in and intends to remain in Los Angeles County, CA.

20. Plaintiff Esperanza Reyes is a California citizen over 18 years of age who resides and intends to remain in Tulare County, CA.

21. Plaintiff Mariaelena Burciaga is a California citizen over 18 years of age who lives in and intends to remain in Fresno County, CA.

22. Plaintiff Stacy Penning is a California citizen over 18 years of age who lives in and intends to remain in Contra Costa County, CA.

23. All Plaintiffs have Meta accounts (*i.e.*, accounts with the social media platforms Facebook or Instagram, both of which Meta owns) and have accessed their accounts from the same browser they used to access the individual Food Bank Defendants' websites.

24. Ms. Timothee has visited the Sacramento Food Bank and Family Services website on many occasions and used the website to access the "Find Food" map, which included entering her home address.

25. Mr. Diep has visited the Los Angeles Regional Food Bank website on many occasions and used the website to access the "Find Food" map, which included entering his home address. In addition, Mr. Diep made calls to the Los Angeles Regional Food Bank through its website and entered his personal information into the website in order to receive emails from the Defendant.

26. Ms. Reyes has visited the Central California Food Bank website on many occasions and used the website to access the "Find Food" map, which included entering her home address. Ms. Reyes has also visited the CalFresh website through the Central California Food Bank website.

27. Ms. Burciaga has visited the Central California Food Bank website on many occasions and used the website to access the "Find Food" map, which included entering her home address. Ms. Burciaga also used the website to help determine her eligibility for CalFresh, which included answering multiple questions to determine the severity of her financial hardship.

28. Mr. Penning has visited the San Francisco Food Bank website on several occasions and used the website to access the "Find Food" map which included answering multiple questions related to his location, age, disability status, mobility status, and urgency of his need for food assistance.

29. All Plaintiffs individually electronically communicated their intent to receive nutrition assistance with only the individual Food Bank Defendants as the intended recipients of such communications.

30. Unbeknownst to Plaintiffs, the Food Bank Defendants allowed Meta to intercept this data, revealing their sensitive financial conditions, and Meta then associated the data with Plaintiffs' Meta accounts and other personal information to target them with advertisements. Indeed, after visiting the Food

Bank Defendants' websites, Plaintiffs received several targeted advertisements related to their sensitive financial information or status.

31. Defendant Meta Platforms, Inc. is a publicly traded Delaware corporation headquartered in Menlo Park, California.

32. Defendant Sacramento Food Bank and Family Services ("SFBFS") is a California 501(c)(3) non-profit organization with its principal place of business in Sacramento, California.

33. Defendant Los Angeles Regional Food Bank ("LAFB") is a California 501(c)(3) non-profit organization with its principal place of business in Los Angeles, California.

34. Defendant Central California Food Bank ("CCFB") is a California 501(c)(3) non-profit organization with its principal place of business in Fresno, California.

35. Defendant San Francisco Food Bank, d/b/a San Francisco-Marin Food Bank ("SFMFB"), is a California 501(c)(3) non-profit organization with its principal place of business in San Francisco, California.

FACTS

I. THE FOOD BANK DEFENDANTS' WEBSITES AND PRIVACY POLICIES

A. Sacramento Food Bank & Family Services

36. SFBFS is a non-profit organization founded in 1976 that serves over 300,000 people in Sacramento County each month. In 2023, its revenue was more than $80.6 million. Its primary customers are those who are in "vulnerable and hard-to-reach groups"[1] and facing food insecurity, often including those who are single mothers, elderly, or disabled.

37. In connection with providing access to food, SFBFS operates the website, sacramentofoodbank.org. This website provides various resources, including eligibility forms and maps to locate local food banks and distribution centers, links to apply for CalFresh, and screeners to determine a user's eligibility for CalFresh benefits. In 2024, SFBFS assisted more than 1,300 individuals with CalFresh applications, opened more than 250 cases for immigrants seeking legal services, and connected a significant number of customers to energy assistance.

[1] *See* https://sacramentofoodbank.org/approach.

38. The SFBFS website does not use a banner consent form or any other mechanism for a user to accept or reject tracking cookies, such as the Pixel. In fact, the Pixel starts transmitting data to Meta the instant a user navigates to the website, without notifying the user.

39. The bottom of SFBFS's webpage links to its Privacy Policy, which states in large font that SFBFS "is intent on protecting the privacy and security of your personal information." It represents users "can use the SFBFS website without telling [it] who you are or revealing any personal information." This representation, however, is false, due to the Pixel's presence on the SFBFS website. Further, the Privacy Policy materially misrepresents and omits information related to how SFBFS transmits users' PII, claiming the "data analytics" that "track [its] users' movements across [its site] . . . for marketing purposes . . . does not include personally identifiable information."

40. These representations and omissions reinforced Plaintiffs' and other Class Members' reasonable belief and expectation that their data related to their personal and sensitive financial information would remain confidential. However, this is false due to the presence of the Pixel on the SFBFS website, which, as discussed further below, contemporaneously links SFBFS users' sensitive communications, PII, and sensitive financial information.

B. Los Angeles Regional Food Bank

41. LAFB is a non-profit organization founded in 1977 that serves over 900,000 people in Los Angeles County each month. In 2023, its revenue was more $261.1 million.[2] Its primary customers are low-income families and persons who are financially vulnerable and facing food insecurity, often including those who are single mothers, elderly, or disabled.

42. In connection with providing access to food, LAFB operates the website, lafoodbank.org. This website provides various resources, including maps to locate local food banks and food distribution centers, links for users to apply to programs such as CalFresh; the Commodity Supplemental Food Program ("CSFP"); food assistance for seniors; the Women, Infants & Children Program; and to access the LAFB's terms and conditions, policies, and information about becoming a donor.

[2] *See* https://lafoodbank.org/about/financials.

43. The website contains a small pop-up on the bottom left of the page purporting to allow users to consent to or decline cookies. However, whether a user allows cookies, *declines them*, or does not interact with the pop-up at all, the Pixel starts tracking and transmitting information to Meta as soon as the user visits any page, such as the Find Food page, beyond the site's landing page.

44. To learn more about what LAFB does with a user's sensitive information, a user must affirmatively navigate to its Privacy Policy page. In its Privacy Policy, LAFB touts itself as being "committed to respecting the privacy of online . . . donors, visitors, volunteers, agency partners and other constituents," and claims its "privacy policy demonstrates the Food Bank's commitment to transparency."[3] The policy represents that LAFB "do[es] not trade, share, rent, or sell any information, personal or otherwise, collected on our website or through any other means," and that "[it] will also never send electronic or physical communications of any kind on behalf of any other organization." However, as discussed further below, the LAFB does allow the Pixel to contemporaneously intercept and transmit users' communications on the LAFB website, and links them with users' PII, including their sensitive financial information. The Policy further omits Meta's exploitation of that sensitive data to sell targeted advertisements.

45. LAFB's representations and omissions reinforced Plaintiff's and other Class Members reasonable belief and expectation that their data related to their personal and sensitive financial information would remain confidential.

C. Central California Food Bank

46. CCFB is a non-profit organization founded in 1992 that serves over 300,000 people each month in Fresno, Madera, Kings, Kern, and Tulare counties. In 2023, its revenue was more than $94.2 million.

47. In connection with providing access to food, CCFB also operates the website, ccfoodbank.org. This website provides various resources, including maps and calendars to locate local food banks and food distribution information; links for users to apply to nutritional assistance programs for low-income individuals such as CalFresh, Groceries2Go, and EBT Sun Buckets; access to CCFB's code of ethics; and information about becoming a donor or volunteer.

[3] https://lafoodbank.org/privacy-policy.

48. The CCFB website does not include a cookie consent banner, pop-up, or any other means of providing information and obtaining consent from users pertaining to the website's use of tracking cookies, including the Pixel. Instead, the only means of disclosing to users what CCFB does with their sensitive information is its Privacy Policy, to which users must affirmatively navigate through a link at the bottom of the webpage.

49. CCFB also has a Code of Ethics, which states that it "safeguard[s] the privacy and confidentiality of [its] clients, volunteers, donors and partners," and "will not take unfair advantage of any professional relationship or exploit others to further [its] personal . . . or business interests."[4]

50. CCFB creates the false impression that it is being forthcoming with its treatment of users' PII, but instead materially misstates how user information is treated, stating:

> We use "cookies" on this site. A cookie is a piece of data stored on a site visitor's hard drive to help us improve your access to our site and identify repeat visitors to our site. For instance, when we use a cookie to identify you, you would not have to log in a password more than once, thereby saving time while on our site. Cookies can also enable us to track and target the interests of our users to enhance the experience on our site. Usage of a cookie is in no way linked to any personally identifiable information on our site."[5]

51. CCFB's Privacy Policy states that, "[w]e take precautions to protect your information. When you submit sensitive information via the website, your information is protected both online and offline." It further states, "[w]hile we use encryption to protect sensitive information transmitted online, we also protect your information offline. Only employees who need the information to perform a specific job (for example, billing or customer service) are granted access to personally identifiable information. The computers/servers in which we store personally identifiable information are kept in a secure environment."

52. The great lengths to which CCFB claims it goes to protect users' data demonstrates that the type of PII its website collects, from users in vulnerable financial situations, is highly sensitive, and reinforces Plaintiffs' and other Class Members' reasonable expectations and belief that their data related to their personal and sensitive financial information would remain confidential.

53. CCFB makes the further false statement in its Privacy Policy that "[w]e are the sole owners of the information collected on this site," and "will not sell or rent this information to anyone." This omits

[4] *See* https://ccfoodbank.org/home/about-us/code-of-ethics.

[5] *See* https://ccfoodbank.org/home/about-us/privacy-policy (emphasis added).

that CCFB shares users' private information with Meta, in real time, via the Pixel; and further omits Meta's contemporaneous interception of user actions and exploitation of that data to sell targeted advertisements.

54. For example, whenever a user clicks to make an appointment to determine their eligibility for, or to enroll in, programs for financially vulnerable individuals via CCFB's website (*i.e.*, via Groceries2Go, CalFresh, or EBT Sun Bucks), Meta intercepts these events.

55. The CCFB website even encourages users to "Share Your Impact" by sharing their personal experience with CalFresh/SNAP programs, programs specifically used by the financially vulnerable, despite its knowledge that the Pixel is contemporaneously tracking and intercepting these events and associating them with users' personal identity as they type out their stories.

D. San Francisco-Marin Food Bank

56. SFMFB is a non-profit organization founded in 1987 that distributes over 1 million meals each week to residents in San Francisco and Marin Counties. It is the largest distributor of food to low-income families and individuals in San Francisco and Marin Counties, and in 2024 delivered weekly groceries to over 8,500 households with "low mobility."[6] Its revenue in the 2023-2024 fiscal year was more than $182.6 million.

57. In connection with providing access to food, SFMFB operates the website sfmfoodbank.org. This website provides various resources, including maps to locate local food banks and food distribution centers, access the Food Bank's terms and conditions, policies, and information about becoming a donor.

58. Although the SFMFB's website contains a consent banner, this banner blends in with the bottom of the homepage and is ineffective as users have no option to reject cookies, only accept them. SFMFB therefore fails to prominently and conspicuously provide a functional disclosure and opportunity to opt out of such tracking on the homepage of its website as statutorily required.

59. Further, even once a user navigates to the Privacy Policy located within this banner, it misrepresents and omits information related to how it treats user data. Under the "Information Sharing" section, the policy states that it "does not sell or rent donor names and addresses with any third parties for any reason other than if compelled by a legal action" yet remains silent about user data. In the section titled

[6] *See* https://sfmfoodbank.org/wp-content/uploads/2025/01/SFMFB-Audited-Financial-Statements_FY2324_Final.pdf.

"Our Commitment to Your Privacy and Security," SFMFB further omits critical information, stating it "will not sell or rent the information you provide to us in any way that has not been specified in our privacy policy."

60. In its section which purports to explain its cookie use, SFMFB only discloses that it "collect[s] the following information about your computer configuration: browser type, operating system, IP address, and the URL of the web page you were on just prior to visiting the Food Bank's website." SFMFB further misrepresents the nature of the Pixel by claiming that "[t]his information will not reveal, nor is it associated with your personal identity."

61. To search for food distribution stations on the SFMFB website, users are required to answer personal questions that reveal a users' location, reasons a user is seeking assistance, their personal health/disability status, age group, and zip code, all of which is intercepted by Meta.

62. Given the Food Banks' representations, omissions, and the sensitivity of medical information and information pertaining to financial hardship and personal food insecurity, users like Plaintiff and other Class Members reasonably expected their data related to this personal and sensitive information to remain confidential.

63. Despite these promises, the SFMFB intentionally incorporated the Pixel into its website, allowing Meta to intercept Plaintiff's and other Class Members' data, including highly sensitive personal, medical, and financial information, in spite of its representations and omissions to the contrary.

64. Thus, SFMFB fails to sufficiently, accurately, and completely inform consumers, like Plaintiff and other Class Members, of the categories of their personal information collected, the purposes for such collection, and whether that information is sold or shared, the categories of third parties to whom it discloses the PII and sensitive financial information to, including but not limited to a link to a Notice of Right to Opt-out of Sale/Sharing. The webpage also fails to feature a conspicuous link or other process that provides users with a simple and easy-to-use method by which to automatically exercise their rights to opt-out of the sale and/or sharing of their data.

65. Further, SFMFB also misrepresents and fails to inform consumers of the additional reasons for which Meta uses their sensitive information, such as associating it with users' personal Meta accounts and then selling that information to third-party advertisers. Thus, Plaintiff and other Class Members' had the

reasonable belief and expectation that their sensitive information and PII would be protected from unauthorized use and disclosure.

II. META'S TRACKING TECHNOLOGY ON THE FOOD BANK DEFENDANTS' WEBSITES

66. In 2024, Meta's annual revenue was a staggering $164.5 billion, a significant increase from its $134.9 billion in revenue the year prior. The vast majority of Meta's revenue, approximately 98%, comes from advertising.

67. Meta's advertising business has been extremely successful due, in large part, to Meta's ability to target people at a granular level. According to Meta's own disclosures, its primary function is to deliver personalized advertisements to users by analyzing their browsing patterns and interactions.

68. Meta's Pixel is a snippet of code that Meta offers for free which is then embedded on a third-party website that tracks a user's activity in real-time as the user navigates through a website. As soon as a user takes any action on a webpage, the Pixel's code embedded in the page re-directs the contents of the user's communication to Meta while the communication between the user and website provider is still occurring.

69. By design, Meta receives the content of website communications as the website user enters or generates the information, but before the website owner receives it.

70. Meta offers the Pixel to companies for free because it benefits Meta. Meta uses the data it gleans from tools like the Pixel to power its algorithms, providing insight into the habits of users across the internet. It also uses this data to target users with advertisements, for which advertisers pay a premium, based on users' interests, thereby increasing Meta's ad revenue.

71. In sum, Meta intercepts and obtains users' personal information via the Pixel for the improper purpose of creating customized audiences for its advertising business.

72. Through this technology, Meta intercepts each page a user visits, what buttons they click, as well as specific information they input into the website, and what they searched. The Pixel sends each of these pieces of information to Meta in real time with users' PII. Meta stores this data on its own servers in California, in some instances, for years. According to Meta:

> You can use the Meta Pixel to track your website visitors' actions also known as conversion tracking. Tracked conversions appear in the Facebook Ads Manager and the Facebook Events Manager, where they can be used to analyze the effectiveness of your conversion funnel and to calculate your return on ad investment. You can also use tracked conversions to define custom audiences for ad optimization and Advantage+ catalog ads campaigns. Once you have defined custom audiences, we can use them to identify other Facebook users who are likely to convert and target them with your ads. . . . Track offsite conversions with your Pixels by adding the fb pixel field to the tracking spec parameter of your ad.[7]

73. The level of personalization is highly granular, with this data often being associated with an individual user's Facebook or Instagram account. For example, if a user is logged into their Facebook or Instagram account when they visit a Food Bank Defendant's website, Meta receives third-party cookies allowing Meta to link the data collected by the Pixel to the specific Facebook or Instagram user.

74. Meta can link PII to individual users by identifying information collected through the Pixel through what Meta calls "Advanced Matching." There are two forms of Advanced Matching: manual matching and automatic matching. Using Manual Advanced Matching, the website developer manually sends data to Meta to link users. Using Automatic Advanced Matching, the Pixel scours the data it receives for recognizable fields, including name and email address, to match users to their Facebook or Instagram accounts.

75. Meta's data collection efforts are not limited to Meta users. Instead, it collects extensive information about individuals who have never had, or no longer have, Facebook or Instagram accounts.

76. If the Pixel collects data about a non-Facebook or Instagram user, Meta still retains and uses the data collected through in its analytics and advertising services, linking those users to "shadow profiles."

77. Indeed, Meta has publicly acknowledged that it uses data from people without Meta accounts (hereinafter "non-users") for a variety of business purposes, including product development, customer analytics reports, and security. These uses alone make it clear that non-user data is essential for Meta's enormous profit.

78. Once data intercepted through the Pixel is processed, Meta makes it available through the "Meta Pixel page" in Events Manager, along with tools and analytics to reach these individuals through

[7] *See* https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking.

future Facebook or Instagram ads. This data can be used to create "custom audiences" to target the user, as well as other Facebook and Instagram users who match that audience's criteria.

79. Here, all Plaintiffs possessed and were logged into their Meta accounts, on the same browser, before accessing the Food Bank Defendants' websites.

80. In addition to using data collected through the Pixel to provide analytics services, Meta uses this data to improve its personalized content delivery, advertising network, and machine-learning algorithms, including by improving its ability to identify and target users.

81. Meta has no way to limit or prohibit the use of data collected through the Pixel given its open systems and advanced algorithms. In fact, after changes to EU privacy laws were ratified in an attempt to stop the surreptitious collection of Internet user data, Meta still publicly assures Pixel clients that they can continue to collect information from EU users without their consent, stating:

> There is no change to how we will process data from people outside the European Region, or data from people in these countries who have allowed the use of cookies. We will continue to attempt to match third-party information shared with us, via Meta Business Tools and APIs, to Facebook accounts. However, we will discard the data of European Region users who have not given, or revoked, consent, except where the individual's data is both: [(1)] Received via our Conversions API or customer list custom audience tool, and [(2)] Matched using contact information, such as email or mobile number, rather than a cookie ID or other device identifier.

82. While Meta has policies in place for website owners to restrict the sharing of sensitive data, Meta knows that this sensitive information is nevertheless being shared with Meta, and usually does not take enforcement actions against companies that it knows are sharing potentially sensitive information with Meta, for good reason: the sensitive information about Plaintiffs and other users is highly valuable.

83. In line with this, Meta has not taken action against any of the Food Bank Defendants despite knowing they are collecting and sharing sensitive user information, since once disclosed to Meta, Meta can sell it to third-party advertisers for its own financial gain.

84. SFBFS uses the Pixel on its website, which tracks and intercepts user interactions, for example, clicks to its food map, often collecting users' home addresses and current locations. SFBFS also uses the Pixel on the page containing its CalFresh inquiry form, asking for, tracking, and transmitting the user's full name, address, phone number, email address, the number of people the user purchases and prepares food for, as well as how many people in the user's household are U.S. citizens. The form also requires the

user to make additional comments, further personalizing and matching the data to the user. The Pixel also intercepts user data on the SFBFS page containing the link to the qualification form for CalFresh, which links users to another website, mRelif.com/screener, also containing the Pixel. This site prompts users to answer questions such as whether they are currently receiving Food Stamps, whether they are age 60 or over, whether they receive disability payments, whether they have less than $4,500 in their bank account, if anyone in their household is pregnant, their total income before taxes in the last thirty days, whether they are a refugee, and their phone number. All of these inputs are tracked and sent to Meta without a user's consent.

85. LAFB uses the Pixel on its website, which tracks and intercepts when users browse the food bank locator interactive map or visit a food distribution location's listing. Meta also intercepts transmissions a user makes, including their sensitive information, when filling out a form to determine their eligibility for CalFresh on the LAFB website, or when making appointments to determine program eligibility.

86. CCFB uses the Pixel on its website, which intercepts user interactions, such as with the "Find Food" map, the food distribution calendar, and pages that help users receive financial support, such as the "Enroll in CalFresh" page and the "Summer EBT Sunbuckets" program for families with school-aged children, among other pages which reveal sensitive information about the user, such as when making appointments or inquiries, which includes asking for users' full names, zip codes, and phone numbers or email addresses.

87. The SFMFB uses the Pixel on its website, which tracks and intercepts user interactions, such as with its food locator, which requires the user to reveal their zip code sensitive medical information about themselves to access, interactions with the appointment calendar for program eligibility which includes asking for an applicant's full name, address, and zip code, and the CalFresh inquiry page.

88. As a result of the Food Bank Defendants' incorporation of the Pixel on their websites, the Food Bank Defendants disclosed, and Meta intercepted, Plaintiffs' and other Class Members' interactions on the Food Bank Defendants' websites, including communications containing their sensitive personal and financial information, and in the case of SFMFB, medical information, often in a non-redacted and non-encrypted form. Meta then subsequently shared, disclosed, and sold this information to third parties without Plaintiffs' or other Class Members' knowledge or consent.

III. PLAINTIFFS AND OTHER CLASS MEMBERS DID NOT CONSENT TO THE FOOD BANK DEFENDANTS' DISCLOSURE OF THEIR SENSITIVE INFORMATION TO META

89. Plaintiffs and other Class Members did not consent to the interception or disclosure of their confidential communications, including sensitive financial and medical information, to Meta. The Food Bank Defendants' disclosure, and Meta's interception of Plaintiffs' confidential communications, PII, and sensitive financial information without their consent is an invasion of privacy and violation of state and federal law.

90. None of the Food Bank Defendants required an opt-in or opt-out for the Pixel's data collection by Plaintiffs or other users before it began tracking and intercepting user data.

91. Plaintiffs and other Class members had no way of knowing that the Food Bank Defendants were disclosing, and Meta was intercepting, their user data including sensitive financial and medical information, when they engaged with the Food Bank Defendants' websites, including using the food locator maps, making appointments, and entering their information into qualification forms, because the software is, almost always, inconspicuously incorporated in the background.

92. This undisclosed conduct is all the more egregious given the nature of the information collected, and the financial and other sensitive statuses of those visiting the websites seeking assistance.

93. Plaintiffs and other Class Members would not expect this information to be disclosed or intercepted without their consent. This is especially true given the Food Bank Defendants' representations that this information would remain private and confidential.

94. Plaintiffs and other Class Members could not consent to Defendants' conduct when they were unaware their confidential communications, PII, sensitive health/disability information, and/or sensitive financial information would be disclosed to and intercepted by Meta.

IV. THE INTRUSION INTO PLAINTIFFS' AND OTHER CLASS MEMBERS' PII, CONFIDENTIAL COMMUNICATIONS, AND SENSITIVE FINANCIAL AND MEDICAL INFORMATION IS HIGHLY OFFENSIVE

95. Plaintiffs and other Class Members have a reasonable expectation of privacy in their data, including sensitive medical and financial information.

96. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares their personal data. A recent study showed that 92% of Americans feel companies should be required to prepare reports on what is done with user data, and that 77% would be likely to support legislation that would prevent companies from selling personal data, with 75% of those who said they like personalized advertising also saying they would support such legislation.[8]

97. The founder of Meta itself, Mark Zuckerberg, knows privacy is important. In 2018, when Mr. Zuckerberg testified before the U.S. Senate Judiciary Committee, he was asked whether he would be comfortable going public with the name of the hotel at which he was staying, or the people he had messaged that week. He answered, "No," and further said, "I think everyone should have control over how their information is used."[9]

98. Despite Americans' concerns about their data being collected and used, a Consumer Reports study found that, from a panel of 709 volunteers who shared archives of their Facebook data, a staggering 186,892 companies sent data about them to the social network. On average, each participant in the study had their data sent to Facebook by 2,230 companies. That number varied significantly, with some panelists' data listing over 7,000 companies providing their data.[10]

99. This level of surveillance is historically unparalleled and is offensive and unconscionable to the reasonable person. This is especially so, as here, where the Plaintiffs' information reveals their need for types of assistance that is seen as shameful by wider society, and puts them in a position to be targeted with predatory ads related to their financial status. Hunger and food insecurity in high-income countries like the United States is caused by a combination of various social inequities such as economic hardship, poor physical and mental health, and other barriers related to the social determinants of health. When examining the relationship between food insecurity and mental well-being, specifically, there is a bidirectional

---

[8] *See* Aliza Vigderman, *Americans Get an F on Digital Privacy Knowledge*, Security.org, Apr. 1, 2025, https://security.org/digital-security/american-digital-privacy-knowledge.

[9] *See* https://nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html.

[10] *See* John Keegan, *Each Facebook User is Monitored by Thousands of* Companies, CONSUMER REPORTS, Jan. 17, 2024, https://consumerreports.org/electronics/privacy/each-facebook-user-is-monitored-by-thousands-of-companies-a5824207467.

association. An individual who is food insecure is more likely to experience poor emotional health, including depression, anxiety, and stress. These factors cause individuals to face social stigma and shame, and these individuals are thus in uniquely vulnerable positions within wider society, which is why those facing food insecurity are often suggested by behavioral health professionals to be treated with special dignity and discretion.[11] Further, ads such as for payday loans, gambling, for-profit education, and other financially predatory businesses are often directed at those who have been categorized as low-income or facing economic hardship, and can even lead to voting discouragement and housing discrimination.[12]

100. Plaintiffs and other Class members were reminded of their hardship and further stigmatized when they were repeatedly targeted with ads directed at exploiting their financial hardships after visiting the Food Bank Defendants' websites.

101. Despite this, Plaintiffs and other Class Members would like to use the Food Bank Defendants' websites again in the future as access to local, affordable food assistance is critical to them but, due to Defendants' unscrupulous data collection and use, feel that they cannot currently trust the websites with their confidential information until the websites no longer use Meta's, or any other tracking software, without adequate, robust disclosures and the opportunity to opt-out of such data sharing.

V. THE DATA PROVIDED TO THE FOOD BANK DEFENDANTS THAT META INTERCEPTED IS PLAINTIFFS' AND OTHER CLASS MEMBERS' PROPERTY, HAS ECONOMIC VALUE, AND ITS ILLICIT DISCLOSURE CAUSED ECONOMIC HARM

102. In 2025, there is a booming and growing economic market for consumers' personal data, including the data the Food Bank Defendants allowed Meta to intercept from Plaintiffs and other Class Members.

103. Selling consumers' personal data is an "extremely profitable business" and "the economic value that can be derived from personal data is immense."[13]

---

[11] *See* Corissa Raymond, MPH & Alexandra Rouzier, *Breaking the Stigma Through Lived Experiences,* BEHAVIORAL HEALTH NEWS, Apr. 18, 2023, https://behavioralhealthnews.org/shame-and-hunger-breaking-the-stigma-through-lived-experiences.

[12] *See* Alvin Chang, *How the Internet Keeps Poor People in Poor Neighborhoods,* VOX, Dec. 12, 2016, https://www.vox.com/2016/12/12/13867692/poor-neighborhoods-targeted-ads-internet-cartoon.

[13] *See* https://datapods.app/blogs/what-your-data-is-actually-worth.

104. In 2022, the global market for data broker services was estimated to exceed $407 billion.[14] Astoundingly, Meta generates *approximately $235 per year from each U.S. user* by leveraging their personal data for targeted advertising.

105. Further, in response to EU privacy regulations, Meta considered charging up to €192 per year for an ad-free version of Facebook and Instagram—effectively assigning a price to the cost of leveraging user data.[15] And although not widely known, consumers can monetize their own PII through platforms such as Neislen Data, Killi, DataCoup, and AppOptix, further underscoring the economic value of user data.

106. All consumers' data is valuable, but the cost of personal data for those with very low incomes—like Plaintiffs and other Class Members who seek food assistance—may be uniquely valuable, and may be uniquely exploitable at users' detriment, such as in regard to their ability to find gainful employment, and thus, to move out of poverty.

107. For example, the use of automated assessment methods to determine "employability" by reviewing information gleaned from social media data giants, like Meta, about job candidates has become a desirable feature of current Applicant Tracking Systems ("ATS"). ATS software is designed to simplify the hiring process and automate the review of resumes and applications for employers, who sometimes face the daunting task of sifting through thousands (or even millions) of applicants, by using highly granular data about workers' behavior both on and off the job, like that collected by Meta, to predict future job performance. As early as 2012, the vast majority of Fortune 500 companies were using some kind of ATS system to screen candidates.[16]

108. Thus, data-driven systems, like those fed by the data intercepted by Meta from the Food Bank Defendants' websites, might contribute to a widening of the income equality gap in the U.S. by providing a ready avenue to prey on the vulnerabilities of low-income people, or to exclude them from opportunities due to biases entrenched in algorithmic decision-making tools. Historically, financially vulnerable Americans have faced much greater surveillance than their wealthier counterparts, and anti-poverty advocates are

---

[14] *Id.*

[15] *Id.*

[16] Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 053 (2017).

rightfully concerned that the digital world, like the challenged behavior here, will replicate, if not reinforce, both covert and overt patterns of surveillance.[17]

CLASS ACTION ALLEGATIONS

109. While reserving the right to redefine or amend the class definition prior to or as part of a motion seeking class certification, including by creating different or additional subclasses, pursuant to Federal Rule of Civil Procedure 23, Plaintiffs seek to represent a Class of all persons in the United States who, at any time during the year preceding the date of the filing of this Complaint to the time a class is notified (the "Class Period"), used one of the Food Bank Defendants' websites. Plaintiff Penning also seeks to represent a Subclass of all persons in the United States who, during the Class Period, used SFMFB's website and indicated their disability status.

110. The Members in the proposed Class (including the Subclass) are so numerous that individual joinder of all Members is impracticable, and the disposition of the claims of the Class in a single action will provide substantial benefits to the parties and Court.

111. Questions of law and fact common to Plaintiffs and the Class include but are not limited to:

a. Whether the Food Bank Defendants collected information about the Class Members;

b. Whether that information constitutes PII or sensitive financial or medical information;

c. Whether that information constitutes messages, reports, or communications under CIPA § 631;

d. Whether the Food Bank Defendants disclosed to Meta the PII or messages, reports, or communications between themselves and other external websites, on the one hand, and Plaintiffs and other Class Members, on the other hand, when Plaintiffs and other Class Members accessed the Food Bank Defendants' websites;

e. Whether Meta read, attempted to read, or learned or used the information it obtained from the Food Bank Defendants about Class Members' use of their websites or external websites such as the CalFresh website;

[17] *Id.* at p. 123.

f. Whether Meta intentionally intercepted Class Members' wires or electronic communications;

g. Whether Meta invaded Class Members' privacy by intercepting their PII or sensitive financial or medical information;

h. Whether the interception, disclosure, use, sharing, and sale of Class Members' sensitive financial data for potentially discriminatory targeted advertising is unconscionable to a reasonable person;

i. Whether the Food Bank Defendants owed a legal duty to Class Members to exercise due care in collecting, using, and safeguarding their PII and sensitive financial information and whether the Food Bank Defendants breached that duty;

j. Whether the Food Bank Defendants adequately and accurately informed Class Members that their PII and sensitive financial information had been disclosed to Meta and used for the benefit of third-parties;

k. Whether the Food Bank Defendants obtained consent or authorization before disclosing to Meta the messages, reports, communications, PII, or sensitive financial information from Class Members;

l. Whether Meta was unjustly enriched;

m. The amount of restitution, damages, punitive damages, and attorneys' fees the Court should award; and

n. What injunctive, equitable, or other relief the Court should award.

112. These common questions of law and fact predominate over questions that affect only individual members of the Class.

113. Plaintiffs' claims are typical of the Class's claims because they are based on the same underlying facts, events, and circumstances relating to Defendants' conduct. Specifically, all Class Members, including Plaintiffs, were subjected to the same violations of privacy as a result of the Food Bank Defendants' disclosure to Meta of their PII or sensitive financial information.

114. Plaintiffs will fairly and adequately represent and protect the interests of the Class, have no interests incompatible with the interests of the Class, and have retained counsel competent and experienced

in class action litigation who will vigorously prosecute this action and otherwise protect and fairly and adequately represent Plaintiffs and the Class.

115. Class treatment is superior to other options for resolution of the controversy because the relief sought for each Class Member is small, such that, absent representative litigation, it would be infeasible for each Class Member to redress the wrongs done to them.

116. Defendants have acted on grounds applicable to the Class, thereby making appropriate final injunctive and declaratory relief concerning the Class as a whole.

117. As a result of the foregoing, class treatment is appropriate under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3).

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Invasion of Privacy Act (CIPA), Cal. Penal Code §§ 630, *et. seq.*

(Against All Defendants)

118. Plaintiffs reallege and incorporate the allegations elsewhere in the Complaint as if set forth fully herein.

119. The California Legislature enacted CIPA finding that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.* § 630. Thus, the intent behind CIPA is "to protect the right of privacy of the people of this state." *Id.*

120. Plaintiffs and Class Members are located in California.

121. Meta is a person for purposes of CIPA.

122. The Food Bank Defendants are persons for purposes of CIPA.

123. The Pixel is a "device" for purposes of CIPA.

124. The Plaintiffs' and Class Members' use of the Food Bank Defendants' websites constitutes "communications" for purposes of CIPA.

125. The Food Bank Defendants and Meta maintain their principal places of business in California, where they designed, contrived, agreed, conspired, effectuated, aided, or received the interception and use of the contents of Plaintiffs' and other Class Members' communications without consent.

CIPA § 631(a)

126. The California State Legislature passed CIPA in 1967 to protect the right to privacy of the people of California.

127. CIPA imposes liability on any person who "by means of any machine, instrument, contrivance, or in any other manner" (1) "intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument," (2) "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within [the state of California]," (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained," or (4) "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section." CIPA requires all-party consent for recording or intercepting communications.

128. Where, as here, a website user or a website developer, owner, or operator is based in California, the message, report, or communication is sent from or received in California.

129. When someone uses a website and enters information on that website, the sole parties to that message, report, or communication are the website user and the website developer, owner, or operator.

130. It is a violation of § 631 to allow someone other than the website user or website developer, owner, or operator to read or learn the contents of messages, reports, or communications between those parties without the consent of all parties.

131. It is a violation of § 631 to read, attempt to read, or learn the contents of messages, reports, or communications between website users and developers, owners, or operators without the consent of all parties.

132. It is a violation of § 631 to use information contained in messages, reports, or communications between website users and developers, owners, or operators without the consent of all parties.

133. It is a violation of § 631 to aid, agree with, employ, or conspire with another to unlawfully read, learn, or use information contained in messages, reports, or communications between website users and developers, owners, or operators without the consent of all parties.

134. Plaintiffs' and other Class Members' use of the Food Bank Defendants' website constitutes messages, reports, or communications between the website user and website developer, owner, or operator. internet communications pass over a wire, line, or cable. Users' messages, reports, and communications on the Food Bank Defendants' websites are thus transmitted and passed over a wire, line, or cable.

135. Meta, using the Pixel, intentionally tapped or made unauthorized connections with the lines of internet communication between, on the one hand, Plaintiffs and other Class Members, and on the other, the Food Bank Defendants' websites, including, where applicable, their CalFresh and CSFP application portals, without the consent of all parties to the communication while this information was in transit.

136. Meta, willfully and without the consent of Plaintiffs and other Class Members, read or attempted to read or learn the contents or meaning of Plaintiffs' and other Class Members' communications with the Food Bank Defendants' website, including, where applicable, the CalFresh portal, while the communications were in transit or passing over any wire, line or cable, or were being received at any place within California. Meta used or attempted to use these communications to help build user profiles, which it then sold to third-party advertisers.

137. Meta knew that the Food Bank Defendants did not have opt-in or opt-out options for cookies on their websites, and collected Plaintiffs' and other Class Members' information in violation of their right to privacy.

138. The Food Bank Defendants employed Meta's Pixel to intercept Plaintiffs' and other Class Members' sensitive financial information and PII, knowing Meta's conduct constituted a breach of duty, and gave substantial assistance to Meta in violating Plaintiffs' and other Class Members' privacy rights.

139. SFBFS did this in a breach of its duty to Plaintiff Timothee and other Class Members because of affirmative representations and omissions made within its Privacy Policy that none of these unlawful acts would occur.

140. LAFB did this in a breach of its duty to Plaintiff Diep and other Class Members because of affirmative representations and omissions made whin its Privacy Policy that none of these unlawful acts would occur.

141. CCFB did this in a breach of its duty to Plaintiffs Reyes and Burciaga and other Class Members because of affirmative representations and omissions made within its Code of Ethics and Privacy Policy that none of these unlawful acts would occur.

142. SFMFB did this in a breach of its duty to Plaintiff Penning and other Class Members because of affirmative representations and omissions made within its Privacy Policy that none of these unlawful acts would occur.

143. Plaintiffs and Class Members have suffered losses due to these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally identifiable information.

144. Pursuant to California Penal Code § 637.2, Plaintiffs and other Class Members have been injured by the violations of California Penal Code § 631, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

CIPA § 632(a)

145. Defendant Meta violated CIPA § 632 when, without their consent, it eavesdropped or recorded confidential communications that Plaintiffs and other Class Members had a reasonable expectation would be kept private. Plaintiffs' and other Class Members' communications were not with a person who the reasonable person knows will likely disseminate the contents of their communications to others, but rather with websites seemingly designed to help those in need, and which had privacy policies that purported to protect the users from the very privacy violations Defendants committed.

146. Plaintiffs and other Class Members had an objectively reasonable belief that the Food Bank Defendants, organizations dedicated to helping those in need, making affirmative representations that they would protect users' privacy, would keep sensitive communications relating to the need to seek nutritional assistance, often due to hardship such as poverty or disability, private. Plaintiffs were unaware Meta was intercepting, profiling, and sharing their sensitive information, and would not have used the Food Bank Defendants' websites, or would have attempted to take actions to prevent the Pixel from intercepting their communications, if they knew.

147. There was not only no express written consent for Plaintiffs' and other Class Members' information regarding their sensitive financial information to be shared, but the Food Bank Defendants also made false representations and warranties that this information would not be collected.

148. Therefore, when it intercepted, read, and shared this sensitive information from the websites' users, Meta was in violation of § 632 of CIPA.

149. When someone violates § 632, the aggrieved party may bring a civil action for $5,000 per violation, pursuant to § 637.2(a)(1). Pursuant to § 637.2(b), the aggrieved party may also seek injunctive relief to enjoin and restrain the violative conduct. Pursuant to § 637.2(c), "it is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

150. Meta and the Food Bank Defendants are liable to Plaintiffs and other Class Members for statutory damages of $5,000 for each time Meta, intentionally and without the consent of all parties to the confidential communications, used the Pixel to eavesdrop upon or record their confidential communications.

CIPA § 635

151. Section 635 of CIPA makes it a crime to "intentionally manufacture[], assemble[], sell[], offer[] for sale, advertise[] for sale, possess[], transport[], import[], or furnish[] to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another." CIPA § 635(a).

152. The Pixel is a device primarily or exclusively designed to eavesdrop upon others' communications because its purpose is to act an invisible add-on to a website, with the intent to collect users' private information for its own use and personal gain, without users' knowledge.

153. Meta designed the Pixel and furnishes it to website owners, including the Food Bank Defendants, to collect user data, including Plaintiffs' and other Class Members' data, which Meta then sells to third- and fourth-party advertisers.

154. Plaintiffs and other Class Members have been injured by Meta's creation and furnishing of the Pixel to the Food Bank Defendants when Meta eavesdropped on their communications with the websites (and third-party websites linked to the websites, such as CalFresh).

155. Meta is liable to Plaintiffs and other Class Members for statutory damages of $5,000 for each time Meta violated this section of CIPA.

CIPA § 638

156. CIPA § 638.51 addresses the unauthorized interception of electronic communications. It prohibits the installation or use of a "pen register," or a "trap and trace device" without first obtaining a court order.

157. Section 638.50(b) defines a pen register as a device or process that records and decodes dialing, routing, addressing or signaling information (often referred to as DRAS) transmitted by a device from which a wire or electronic communication is sent.

158. Section 638.50(c) defines a trap and trace device as one that captures incoming electronic or other impulses to identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication.

159. The Meta Pixel tracking tool is a device or process because it is software that identifies consumers, gathers data, including addressing information (such as IP addresses, PII and sensitive financial information), contents of users' communications, and correlates those contents with that data. The Pixel also runs on computing devices. Thus, the Meta Pixel falls under the definition of a pen register or trap and trace device for purposes of this statute.

160. Neither Meta nor the Food Bank Defendants requested or received a court order before installing, and allowing to be installed, the Pixel's code onto the websites, and Plaintiffs and other Class Members did not consent to and had no knowledge of the use of the Pixel device on the Food Bank Defendants' websites before their electronic communications were intercepted.

161. Pursuant to Cal. Penal Code § 637.2(a)(1), Meta is liable to Plaintiffs and Class Members for statutory damages of $5,000 for each time Meta violated this section of CIPA.

SECOND CAUSE OF ACTION

Violation of the Federal Wiretap Act, 18 U.S.C. § 2510 *et. seq.*

(Against Meta)

162. Plaintiffs reallege and incorporate the allegations elsewhere in the Complaint as if set forth fully herein.

163. The Wiretap Act prohibits the intentional "interception" of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1).

164. The unauthorized transmission of data between Plaintiffs and other Class Members, on the one hand, and the websites on which the Pixel tracked and intercepted their communications, on the other, were "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

165. Using the Pixel, Meta intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications in which they had a reasonable expectation of privacy, for unauthorized and improper purposes, which resulted in the tortious acts alleged herein.

166. Plaintiffs and other Class Members did not consent to the interception of their communications because they were not notified of the practice at issue, nor could they have consented because they were unaware of Meta's interceptions, which occurred concurrently as Plaintiffs and other Class Members used the Food Bank Defendants' websites.

167. Meta's actions in intercepting and tracking user communications were intentional. Meta is aware that it is intercepting communications related to Plaintiffs' and other Class Members' sensitive financial information, and in the case of SFMFB, medical information, but in these circumstances but has taken no remedial action.

168. Meta was never a party to any of the communications sent and received by Plaintiffs and other Class Members. Thus, its purpose was and is to intentionally and undetectably intercept contents of Plaintiffs' and Class Members' electronic communications of PII and sensitive financial and medical information while interacting with the Food Bank Defendants' websites, in violation of this statute.

169. Plaintiffs and the Class suffered harm as a result of Meta's violations of the Wiretap Act, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate; (b) the sum of actual damages suffered and the profits obtained by the Defendant as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater; (c) punitive damages; and (d) reasonable costs and attorneys' fees.

THIRD CAUSE OF ACTION

Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion

(Against All Defendants)

170. Plaintiffs reallege and incorporate the allegations elsewhere in the Complaint as if set forth fully herein.

171. Plaintiffs and other Class Members have reasonable expectations of privacy in using the Food Bank Defendants' websites, and in particularly in their PII and sensitive financial and medical information. The reasonable expectation of privacy in their sensitive financial information is intrinsic and further stems from and is reinforced by representations made by the Food Bank Defendants.

172. The Food Bank Defendants' disclosure of Plaintiff's and other Class Members' sensitive PII and confidential communications, including their names, email addresses, phone numbers, private information entered into forms, financial statuses, gender or disability statuses, ages, applications to CalFresh and other programs designed to help disadvantaged groups, and other sensitive information—including, for Defendant SFMFB, sensitive medical information—to Meta, constitutes an intentional intrusion upon Plaintiffs' and Class Members' solitude or seclusion because the Food Bank Defendants disclosed this data, and Meta intercepted this data that was intended to stay private, without the users' consent.

173. Plaintiffs and other Class Members had a reasonable expectation of privacy in their PII and a reasonable expectation that while using the Food Bank Defendants' website, their sensitive information would not secretly be intercepted without their consent, including information regarding their medical or financial status and other sensitive personal details, because this type of information is inherently sensitive, and because of the Food Bank Defendants' representations. Plaintiffs and other Class Members reasonably expected this information would remain private and confidential and would not be disclosed to third parties without their consent.

174. Moreover, the Food Bank Defendants' statuses as non-profit organizations further adds to Plaintiffs' and other Class Members' reasonable belief that their private information would be protected and not given freely to a multibillion-dollar advertiser to use for its own profit.

175. The surreptitious taking and disclosure of Plaintiffs' and other Class Members' PII, including sensitive financial and, in the case of SFMFB, medical information, from thousands of vulnerable individuals

seeking food assistance, was and is highly offensive to the reasonable person because it violated and violates expectations of privacy that have been established by social norms.

176. The offensiveness of this conduct is all the more apparent because the Food Bank Defendants' disclosure of this information was conducted despite their affirmative representations that website users' privacy is important to them and protected, and in a manner that Plaintiffs and other Class Members were unaware of, through the virtually undetectable incorporation of Meta's Pixel into their websites. This is a violation of the trust of vulnerable individuals seeking assistance.

177. Accordingly, the Food Banks' disclosure and Meta's interception of Plaintiffs' and other Class Members' PII and confidential communications, including sensitive medical and financial data, would be, and is highly offensive to a reasonable person.

178. As a result of Defendants' actions, Plaintiffs and other Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights. Plaintiffs and other Class Members have been damaged as a proximate and direct result of the Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

179. Plaintiffs seek appropriate relief for that injury, including but not limited to damages in a sum to be determined at trial that will reasonably compensate Plaintiffs and other Class Members for the harm to their privacy interests, as well as a disgorgement of profits made by the Meta as a result of its intrusions upon Plaintiffs' and other Class Members' privacy, and destruction of any information obtained as a result of their past intrusions.

FOURTH CAUSE OF ACTION

Violation of the California Constitutional Right to Privacy, Cal. Const. Art. 1 § 1

(Against All Defendants)

180. Plaintiffs reallege and incorporate the allegations elsewhere in the Complaint as if set forth fully herein.

181. ART. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

182. Plaintiffs and other Class Members possess a legally protected privacy interest in their PII and sensitive financial and medical information and due to the inherently sensitive nature of their information and the Defendant Food Banks' websites' representations, had a reasonable expectation of privacy in this PII and sensitive information.

183. Plaintiffs' and other Class Members' private affairs include their PII and their sensitive financial and medical information that Meta captures from eavesdropping on Plaintiffs and Class Members' private communications with the Food Bank Defendants' websites and other third-party websites linked to the Food Bank Defendants' websites.

184. Meta, with the cooperation of the Food Bank Defendants, intentionally intruded on and into Plaintiffs' and other Class Members' private affairs by intentionally capturing their PII and other sensitive information. These intrusions are highly offensive to a reasonable person.

185. Societal expectations and laws created a duty Meta and the Food Bank Defendants owed to Plaintiffs and other Class Members to protect and respect their privacy. Meta breached that duty by implementing a system that eavesdrops on private communications and captures the PII of Plaintiffs and other Class Members without their consent, and without legitimate justification. The Food Bank Defendants breached that duty by knowingly implementing the pixel on their webpages.

186. Meta's conduct described herein violated Plaintiffs' and other Class Members' right to privacy, as guaranteed by ART. 1, § 1 of the California Constitution. Meta's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and other Class Members.

187. The Food Bank Defendants' conduct described herein violated Plaintiffs' and other Class Members' right to privacy, as guaranteed by ART. 1, § 1 of the California Constitution. Meta's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and other Class Members.

188. As a result, Plaintiffs and other Class Members seek injunctive relief prohibiting any further intrusions into their privacy by Defendants, the destruction of any information obtained from Plaintiffs and other Class Members as a result of their past intrusions, and damages in a sum to be determined at trial.

FIFTH CAUSE OF ACTION

Negligence

(Against the Food Bank Defendants)

189. Plaintiffs reallege and reincorporate the allegations elsewhere in the Complaint as if set forth fully herein.

190. The Food Bank Defendants owed to Plaintiffs and other Class Members, who trusted and believed that their data and PII would not be disclosed without their consent, a duty of care.

191. In violation of that duty, the Food Bank Defendants negligently, carelessly, recklessly or unlawfully transmitted to and permitted Meta to access Plaintiffs' and other Class Members' PII and sensitive financial and, in the case of SFMFB, medical information.

192. As a direct and legal result of the Food Bank Defendants' lack of reasonable care in handling Plaintiffs' PII and sensitive medical and financial information and wrongful conduct and omissions, Plaintiffs and other Class Members have sustained foreseeable harm and damages in a sum to be determined at trial.

SIXTH CAUSE OF ACTION

Violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et. seq.*

(Against Defendant SFMFB)

193. Plaintiff Penning realleges and incorporates the allegations elsewhere in the Complaint as if set forth fully herein.

194. SFMFB is a "business" for purposes of the CCPA.

195. Plaintiff Penning's and other Class Members' disability status is "medical information" for purposes of the CCPA. Cal. Civ. Code § 1798.81.5(d)(2).

196. "Medical information" is "personal information" for purposes of the CCPA. Cal. Civ. Code § 1798.81.5(d)(1)(iv).

197. The CCPA grants California residents rights to control their personal information, such as the right to limit the use of the sensitive information collected about them, and dictates that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected." Cal. Civ. Code § 1798.81.5(a)(1). It also dictates that "a business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected

and the purposes for which [that] information is collected, and whether that information is sold or shared." *Id.* § 1798.100(a)(1). And it provides that "[a] third party shall not sell or share personal information about a consumer that has been sold to, or shared with, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out." *Id.* § 1798.115.

198. When Plaintiff Penning answered the questions required to view the "Find Food" map on the SFMFB website, he revealed his medical history pursuant to the CCPA when he interacted with boxes requiring him to indicate whether he is "an adult living with disabilities" and/or "ha[s] a disability that makes it difficult to leave home to get food."

199. Through the Pixel, SFMFB wrongly and knowingly collected, used, and transmitted Plaintiff Penning's and other Class Members' non-encrypted and non-redacted PII and sensitive medical information to Defendant Meta, who then used and sold this information to third parties without their consent or authorization; and those parties in turn used the data for their own benefit without providing Plaintiff or other Class Members the explicit notice or opportunity to exercise their rights to opt out of such actions, as required under the CCPA.

200. Disclosing Plaintiff's and other Class Members' PII and sensitive medical information to Defendant Meta was not reasonably necessary or proportionate to perform the services that SFMFB performed, or that Plaintiff and other Class Members received.

201. By collecting, using, and sharing Plaintiff's and other Class Members' PII and sensitive medical information to Meta without providing notice, sufficient opt-out opportunities, or obtaining consent, Defendants violated the CCPA, and Plaintiffs and the Class are entitled to injunctive relief.

202. Pursuant to Ca. Civ. Code § 1798.150(b), Plaintiff sent SFMFB notice of its violation and of his CCPA claims. If SFMFB fails to cure its tortious business practices, Plaintiff shall seek leave to amend the Complaint to add claims for monetary relief, including statutory and actual damages under the CCPA. As of the date of this filing, the Defendant has not cured the CCPA violations.

SEVENTH CAUSE OF ACTION

Unjust Enrichment

(Against Meta)

203. Plaintiffs reallege and incorporate the allegations elsewhere in the Complaint as if set forth fully herein.

204. Meta has wrongfully and unlawfully trafficked in Plaintiffs' and other Class Members' personal information and other personal data without their consent for substantial profits.

205. Plaintiffs and other Class Members have an equitable, legal, and financial interest in their PII and sensitive financial information, and conferred an economic benefit on Meta in the form of profits resulting from the use of their PII and sensitive financial and medical information to improve Meta's marketing efforts and financial position, including through targeted advertising.

206. Meta's financial benefits resulting from its unlawful and inequitable conduct are economically traceable to Plaintiffs' and other Class Members' PII and sensitive financial and medical information being obtained without their consent.

207. Plaintiffs and other Class Members have been injured because they have not been compensated for the benefits they conferred on Meta. Plaintiffs and other Class Members' legal remedies are inadequate to address this injury.

208. It would be inequitable, unconscionable, and unjust for Meta to retain these economic benefits because the benefits were procured as a direct and proximate result of its wrongful conduct.

209. Plaintiffs and other Class Members accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that Meta obtained as a result of its unlawful and wrongful conduct.

PRAYER FOR RELIEF

210. Wherefore, Plaintiffs, individually and on behalf of the proposed Class, pray for judgment as follows:

a. An Order declaring this action to be a proper class action, appointing Plaintiffs as Class Representatives, and appointing Plaintiffs' undersigned counsel as Class Counsel;

b. An Order requiring Defendants to bear the cost of Class Notice;

c. An Order requiring Defendants to pay statutory, compensatory, and punitive damages as permitted by law;

d. An Order enjoining Defendants from disclosing the PII of Food Bank Defendant website users without their informed, written consent obtained in a manner consistent with 18 U.S.C. § 2710(b)(2)(B);

e. An Order requiring Defendants to pay restitution to restore all funds acquired by means of any act or practice declared by this Court to be an unlawful or unfair business act or practice;

f. An Order enjoining the Food Bank Defendants from allowing Meta to intercept, learn the contents of, and profit from private communications between the Food Bank Defendants and users of its website without the users' consent;

g. An Order enjoining Meta from intercepting, learning the contents of, and profiting from private communications between the Food Bank Defendants and users of their websites without the users' consent;

h. An Order compelling Meta to destroy all PII obtained from the Food Banks and to comply with 18 U.S.C. § 2702(e);

i. A judgment awarding any and all further equitable, injunctive, and declaratory relief as may be appropriate;

j. Pre- and post-judgment interest, as permitted by law;

k. An award of attorney fees and costs; and

l. Such further relief as the Court deems necessary, just, or proper.

JURY DEMAND

211. Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: June 17, 2025

/s/ Jack Fitzgerald

FITZGERALD MONROE FLYNN PC
JACK FITZGERALD
jfitzgerald@fmfpc.com
MELANIE R. MONROE
mmonroe@fmfpc.com
TREVOR FLYNN
tflynn@fmfpc.com

PETER GRAZUL
pgrazul@fmfpc.com
ALLISON FERRARO
aferraro@fmfpc.com
2341 Jefferson Street, Suite 200
San Diego, California 92110
Phone: (619) 215-1741
Counsel for Plaintiffs